B. E.

Third Semester Examination, May-2008

DIGITAL & ANALOG COMMUNICATION

Note : Attempt any five questions. All questions carry equal marks.

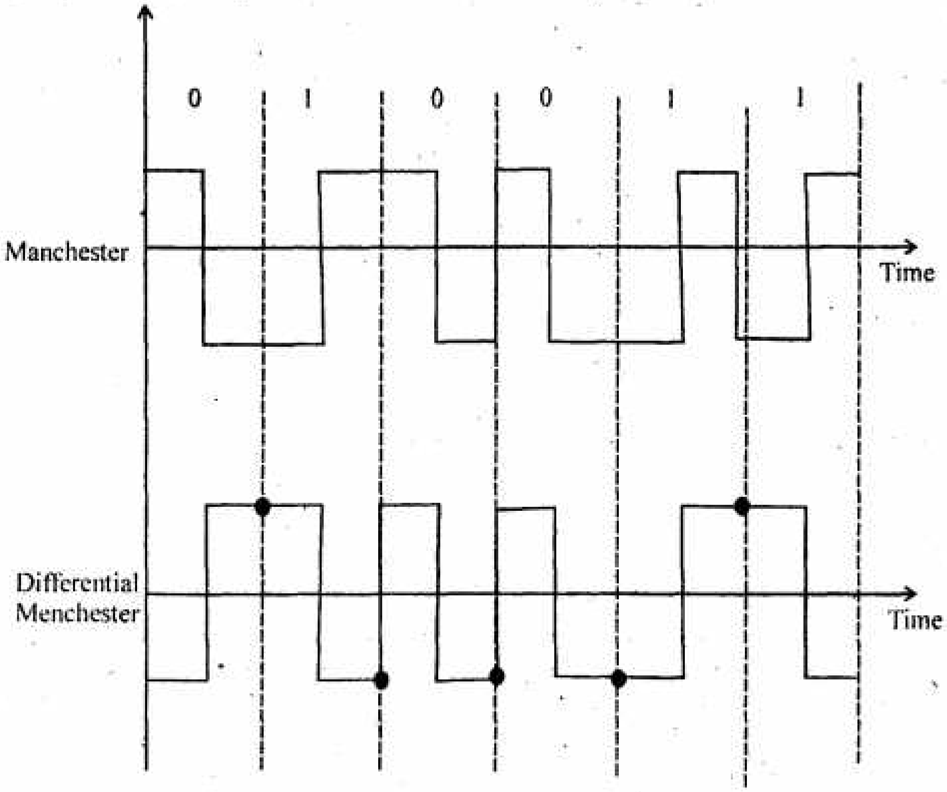
Q. 1. Consider the Gaussian pulse :

$$g(t) = \frac{1}{\sqrt{2\pi\tau}} \exp\left(\frac{\pi t^2}{2\tau^2}\right)$$

The parameter τ provides one possible measure for the duration of the pulse. Defining the BW of pulse, show that the time BW products is 1/4.

Q. 2. Write in detail about the Differential Manchester encoding.

Ans.



Manchester & D differential Manchester Schemes

The idea of RZ (Return to zero) (transition at the middle of the bit) & the idea of NRZ (non-return to zero level) are combined into the Manchester schemes. In Manchester encoding, the duration fo the bit is divided into two levels in the second half. The transition at the middle of the bit provides synchronization. Differential Manchester on the other hand, combines the idea fo RZ & NRZ-I (non-return to zero-invest). There is always a transition at the middle of the bit, but the bit values are determined at the beginning of the bit. If the next bit is 0, there is a transition; if the next bit is 1, there is none. Fig. 10, shows both Manchester & differential Manchester encoding.

o = No inversion : next bit is 1

● = Inversion : next bit is 0.

The Manchester schemes overcomes several problems associated with NRZ-L, & differential Manchester overcomes several problems associated with NRZ-1. First, there is no base line condering. There is no DC component because each bit has a positive & negative voltage contribution. The only drawback is the signal rate. The signal rate for Manchester & differential Manchester is double that for NRZ. The reason is that there is always are transition at the middle of the bit & may be one transition at the end of each bit. The Manchester & Differential Manchester encoding schemes are also called biphase schemes.

Q. 3. Write about the various transmission media and derive the expression for Shannon limit on data rate.

Ans. Transmission Media :

A transmission media can be broadly defined as anything that can carry information from a source to a destination. For e.g. the transmission medium for two people having a dinner conversion is the air. The air can also be used to convey the message in a smoke signal or semaphore. For a written message, the transmission medium might be a mail carrier a truck or an airplane.

In telecommunications, transmission media can be divided into two broad category:

1. Guided Media (Wired)

(i) Twisted pair cable.

(ii) Coaxial cable.

(iii) Fibre optic cable

2. Unguided Media (wireless)

Free space :

1. Guided media :

Guided media, which are those that provide a conduit from one device to another, include twisted pair cable, coaxial cable, & fibre optic cable. A signal traveling along any of these media is directed & contained by the physical limits of the medium. Twisted pair & coaxial cable use metallic (copper) conductors that accept is transport signals in the form of electric current. Optical fibre is a cable that accepts & transports signals in the form of lights.

2. Unguided media :

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space & thus are available to anyone who has a device capable of receiving them.

Shannon capacity :

In reality we cannot have a noiseless channel; the channel is always noisy. In 1994 claude Shannon introduced a formula, called the Shannon capacity, to determine the theoretical highest data rate for a noisy channel.

$$\boxed{\text{Capacity} = \text{bandwidth} \times \log_2(1+\text{SNR})}$$

In this formula, bandwidth is the bandwidth of the channel, SNR is the signal to noise ratio, & capacity is the capacity of the channel in bits per second. In the Shannon formula there is no indication of the signal level, which means that no matter how many levels we have, we cannot achieve a data rate higher than the capacity of the channel. In other words, the formula defines a characteristics of the channel, not the method of transmission.

Q. 4. Explain the sliding window protocol.

Ans. In this protocol, the sliding window is an abstract concept that defines the range of sequence nos. That is the concern of the sender & receiver. The range which is the concern of the sender is called the send sliding window; the range that is the concern of the receivers called the receive sliding window.

The send window is an imaginary box covering the sequence nos. of the data frames which can be in transit. In each window position, some of these sequences no. Define the frames that have been sent; others define those that can be sent.

The window at any time divides the possible sequence numbers into four regions as shown in fig. (9).

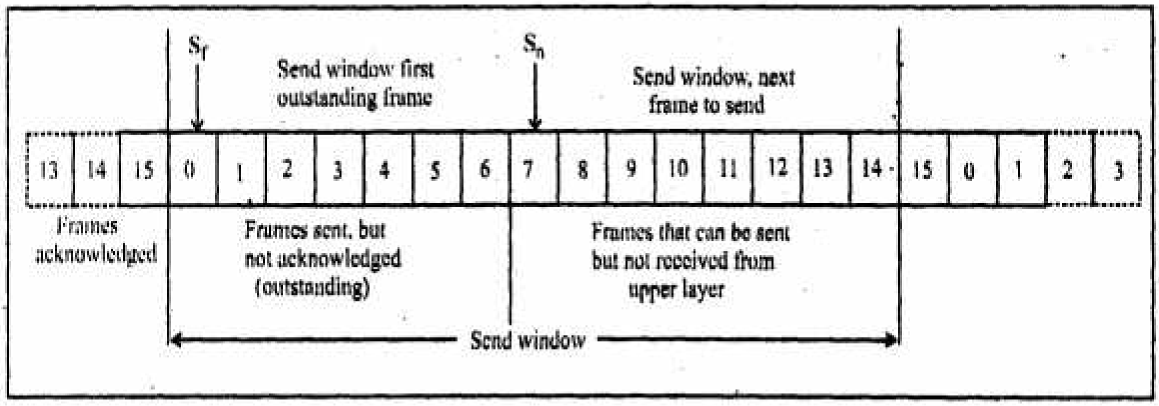
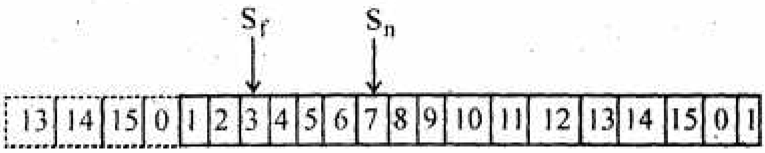

S_f
Send window first outstanding frame
S_n
Send window, next frame to send
13
14
15
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
0
1
2
3
Frames acknowledged
Frames sent, but not acknowledged (outstanding)
Frames that can be sent but not received from upper layer
Send window

Fig. 9. Sent window for Go back-N ARQ.

The first region, from the far left to the left wall of the window, defines the sequence numbers belonging to frames that are already acknowledge. The sender does not worry about these frames & keeps no copies of them. The second region, define the range of sequence nos. Belonging to the frames that are sent & have an unknown status. The third range, defines the range of sequence nos. for frames that can be sent. Finally, the fourth region, defines sequence nos. That cannot be used until the window sliders.

The window itself is an abstractions; three variables defines its size & location at anytime. We call these variables S_F (sent window, the first outstanding frame), S_N (send window, the next frame to be sent); and S_{size} (send window size). The variable S_F defines the sequence number of the first (oldest) outstanding frame. The variable S_N holds the sequence number that will be assigned to the next frame to be sent. Finally, the variable S_{size} defines the size of the window, which is fixed in our protocol.

Fig. Shows send window after sliding.



Above fig., shows how a send window can slide our or more slots to the right when an acknowledgment arrives from the other end. The acknowledgment in this protocol are cumulative, meaning that more than are frame can be acknowledged by an ACK frame. In fig. frames 0, 1 is 2 are acknowledge, so the window has slide to the right three slots. The value of S_F is 3 because frame 3 is now the first outstanding frame.

The receive window makes sure that the correct data frames are received as that the correct acknowledgments are sent. The size of the receive window is always. The receiver is always looking for the arrival of a specific frame. Any frame arriving out of order is discarded & resent.

Q. 5. Explain ISDN and compare it with PK, others like PSTN, Asynchronous Digital Subscriber line.

Ans.

Q. 6. Write in detail about the steps involved in public key cryptography.

Ans. Public key cryptography (asymmetric key cryptograph) :

The public key cryptography is basically known as asymmetric key cryptography.

In asymmetric or public key cryptography, there are 2 keys; a private key is a public key. The private key is kept by the receiver. The public key is announced to the public. Suppose a user Alice wants to send a message to Bob (second user). Alice uses public key to encrypt the message. When the message is received by Bob, the private key is used by the Bob to decrypt the message.

In public key encryption/decryption, the public key that is used for encryption is different from the private key that is used for decryption. The public key is available to the public; the private key is available only to an individual.

In asymmetric key cryptography we uses either of the 2 algorithms i.e. RSA or Diffie-Hellman.

1. RSA (Rivest, Shamir & Addeman Algorithm) :

The most common public key algorithm is RSA, named for its inventors (Rivest, shamir & addeman). It uses 2 nos. e and d, as the pubic is private keys.

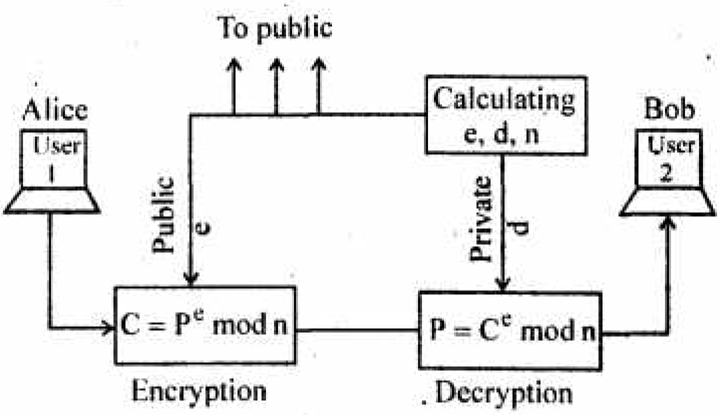


Fig. 7. Shows RSA algorithm process.

Selecting Keys :

Bob use the following steps to select the private is public keys :

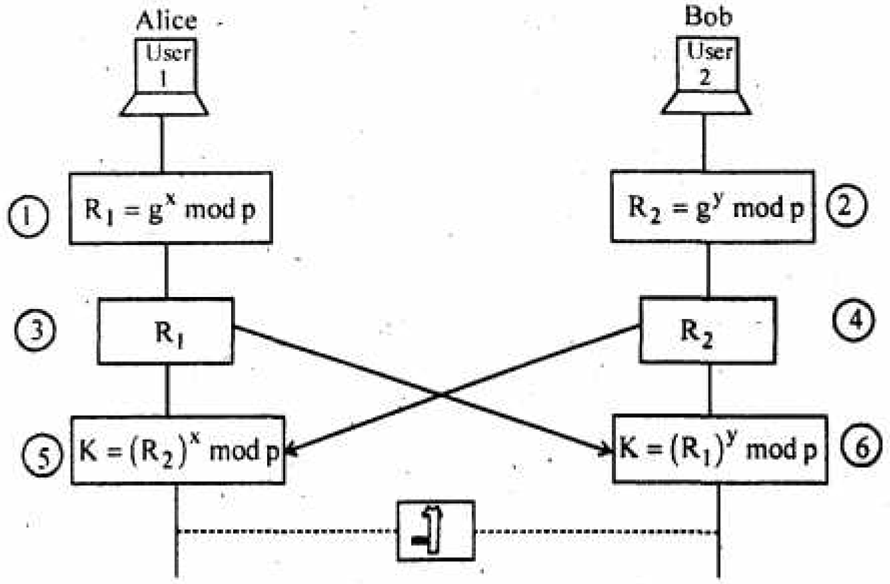
1. Bob chooses two very charge prime nos. p & q. Remember that a prime no. is one that can be divided evenly only by 1 & itself.
2. Bob multiplies the above 2 primes to find n, the modules for encryption is decryption. In other words, $n = p \times q$.
3. Bob concludes another no $\phi = (p-1) \times (q-1)$.
4. Bob chooses a random integer e. He then calculates d so that $d \times e = 1 \bmod \phi$.
5. Bob announces e & n to the public; he keeps v & d secret.

2. Diffie-Helmann Algo :

Diffie-Helmann was originally designed for key exchange. In this process the steps are as follows :

1. Alice chooses a large random number x is calculates $R_1 = g^x \bmod \rho$.

Fig. (8) Diffie-Hellman method :



Step 2 : Bob choices another large random number y is calculates $R_2 = g^y \bmod \rho$.

3. Alice sands R_1 to Bob. Alice does not sent he value of x, she sends only R_1.

4. Bob sends R_2 to Alice. Again he sends only R_2.

5. Alice calculates $K = (R_2)^x \bmod \rho$.

6. Bob also calculates $K = (R_c)^y \bmod p$.

The symmetric key for the session is k.

$$\boxed{(g^x \bmod p)^y \bmod p = (g^y \bmod p)^x \bmod p = g^{xy} \bmod p}$$

Bob has calculated $K = (R_1)^y \bmod p = (g^x \bmod p)^y \bmod p = g^{xy} \bmod p$. Alice has calculated $K = (R_2)^x \bmod p = (g^y \bmod p)^x \bmod = g^{xy} \bmod p = (g^y \bmod p)^x \bmod = g^{xy} \bmod p$.

Both have reached the same value without Bob knowing the value of x is without Alice knowing the value of y.

Q. 7. Explain about the various framing methods in Data Link Layer.

Ans. Framing : Framing is data link layer separates a message from one source to a destination or from other messages to other destinations, by adding a sender address is a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt. Framing is of two types.

1. Fixed size framing :

Frames can be fixed or variable size. In fixed size framing, there is no lead for defining the boundaries of the framẽs; the size itself can be used as a delimiter. An ex. of this type of framing is the ATM wide area network, which uses frames of fixed size called cells.

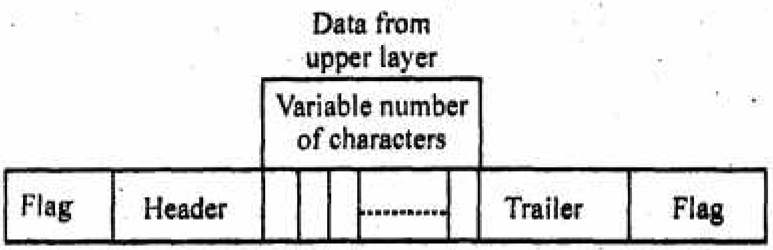
2. Variable size framing :

In variable size framing, we need a way to define the end fo the frame is the beginning of the next. There are two approaches for this purpose.

(i) Character oriented protocols :

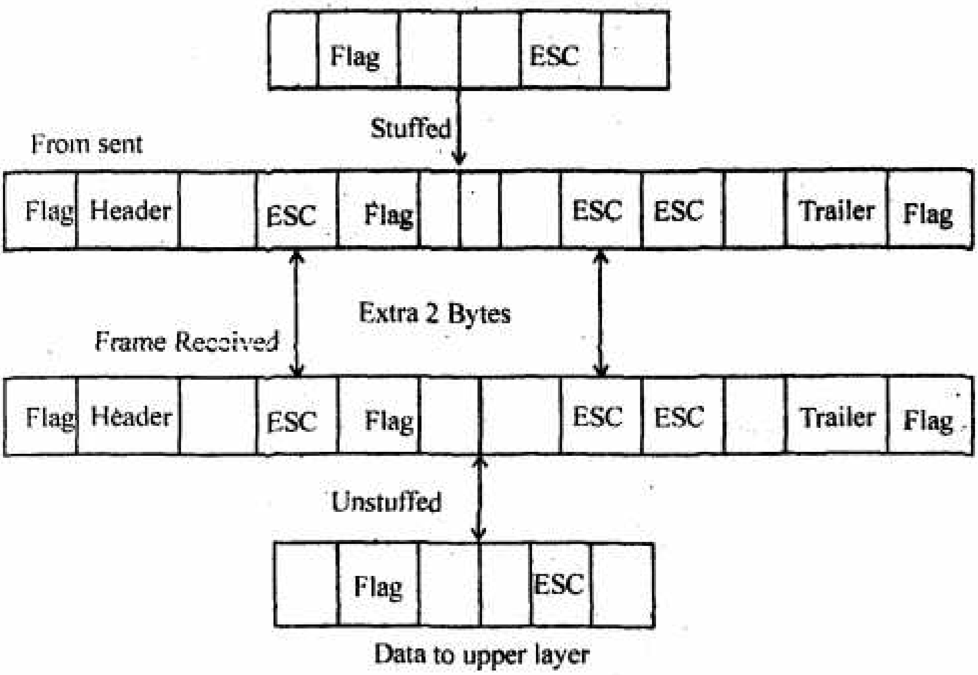
In a character oriented protocol, data to be carried are 8 bit characters from a coding system such as ASCII. The header, which normally carries the source is destination address is other control information, is the trailer, which carries error detection or error correction redundant bits are also multiples of 8 bits. To separate one from the next, an 8 bit (1 byte) flag is added at the beginning is the end of a frame. The flag, composed of protocol dependent special characters, signals the start or end of a frame.

Fig. Shows the format of a frame in a characters oriented protocol.



The flag could be selected to be any character not used for text communication. Now, we send other types of information such as graphs, audio is video. Any pattern used for the flag could also be part of the information. If this happens, the receiver, when it encounters this pattern in the middle of the data, thinks it has reached the end of the frame. To fix the problem, a byte-stuffing strategy was added to character oriented framing. In byte-stuffing, a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section is treats the next character as data, not a delimiting flag.

Fig. Shows the situation :



(ii) Bit-oriented protocol : In a bit oriented protocol the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphics, audio, video & so on. However in addition to headers. We still head a delimiter to separate one from the other. Most protocols use a special 8 bit pattern flag 01111110 as the delimiter to define the beginning & the end of the frame as shown in fig. 3.

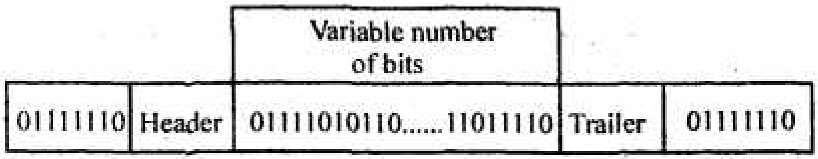
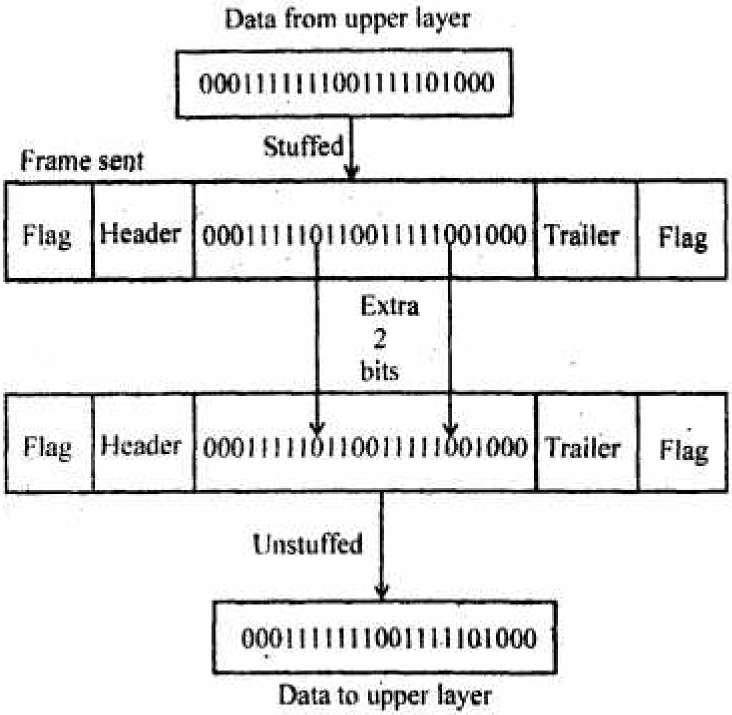


Fig. 3. A frame in a bit oriented protocol.

It also creates a same problem as byte oriented protocol. i.e., if the flag pattern appears in the data, we need to somehow inform the receiver that this is not the end fo the frame. We do this by stuffing 1 single bit (instead of 1 byte) to prevent the pattern from looking like a flag. The strategy is called bit stuffing. In bit stuffing, it a 0 is 5 consecutive (bits are encountered, an extra 0 is added. This extra stuffed bit is eventually removed from the data by the receiver. Note that the extra bit is added after one 0 followed by 5 is regardless of the value of the next bit. This guarantees that the flag field sequence does not inadventually appear in the frame. Fig., (4) shows the situation :



Q. 8. Write notes on the following :

(i) CRC,

(ii) Virtual circuits.

Ans. (i) CRC : CRC (Cyclic Redundancy Check) :

CRC is used in the networks such as LAN's & WAN's. When can create cyclic codes to correct errors. Cyclic codes are special linear block codes with one extra property. In a cyclic code, if a codeword is cyclically shifted, the result is another codeword.

Table (1) Shows CRC code with C(7,4).

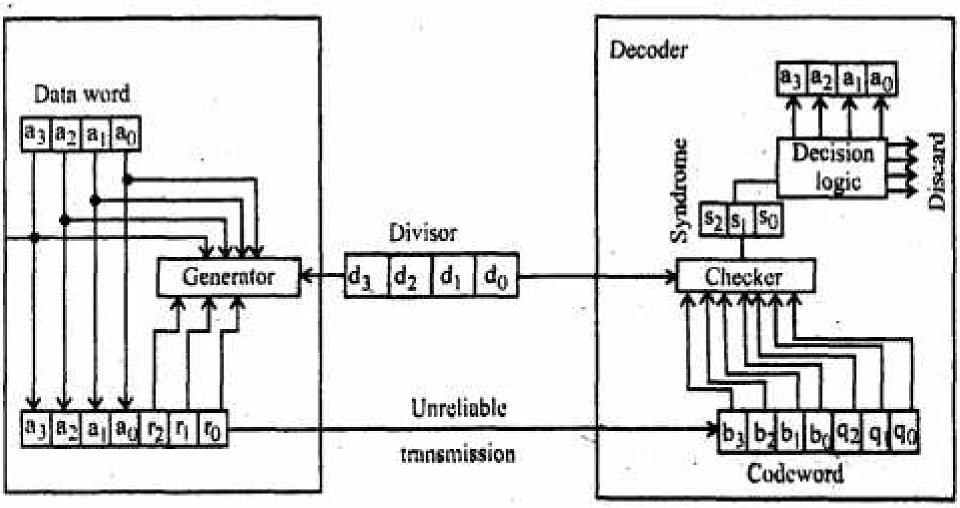
Here it shows an eg.., of a CRC code in which it shows both linear is cyclic properties of this code :

Data word	Code word	Data word	Code word
0000	0000000	1000	1000101
0001	0001011	1001	1001110
0010	0010110	1010	1010011

0011	0011101	1011	1011000
0100	0100111	1100	1100010
0101	0101100	1101	1101001
0110	0110001	1110	1110100
0111	0111010	1111	1111111

Fig. 6. Shows one possible design for the encoder is decoder.

Fig. 6. CRC Encoder is Decoder :



In the encoder the dataward has k bits (4 here); the codeword has n bits (7 here). The size of the dataword in argumented by adding n-k (3 here). Os to the right hand side of the word. The n bit result is fed into the generator. The generator uses a divisor of size $n-k+1$ (4 here), predefined as agreed upon. The generator divides the argument dataword by the divisor. The quotient of the division is discarded; the remainder $(r_2\, r_1 r_0)$ is appended to the dataword to create the codeword.

The decoder receives the possibly corrupted codeword. A copy of all n bits is fed to the checker which is a replica of the generator. The remainder produced by the checker is a syndrome of n-k (3 here) bits, which is fed to the decision logic analyser.

The analyzer has a simple function. If the syndrome bits are all Os, the left most bits of the codeword are accepted as the dataword (interpreted as a no error); otherwise the 4 bits are discarded (error).

(ii) Virtual circuits :

Connection between 2 end points is accomplished through transmission paths (TP), virtual paths (VP) is virtual circuits (VCs).

Transmission path (TP) is the physical connection (wire, cable, satellite etc. between an endpoint is a switch or between 2 switches.

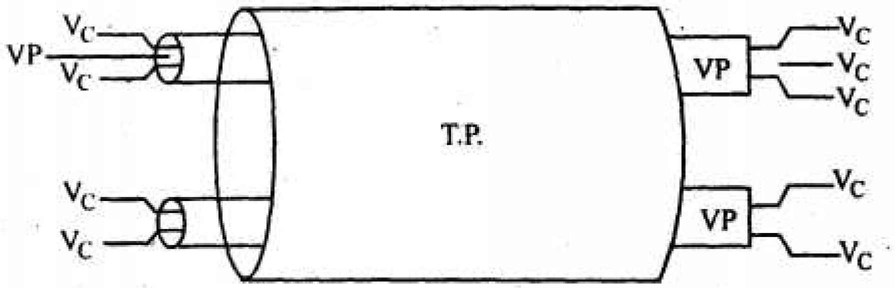
A transmission path is divided into several virtual paths.

A virtual path (VP) provides a connection or a set of connections between two switches. Think of virtual path as a highway that connects 2 cities.

Cell network are based on virtual.

Circuits (VC) :

All cells belonging to a single message follow the same virtual circuits remain in their original order until they reach their destination. Think of a virtual circuits as the values of a highway (virtual path). Fig. 5. Shows the relationship between a TP, VP is VC that logically connects two points.


VP
V_C
V_C
V_C
V_C
T.P.
VP
V_C
V_C
V_C
VP
V_C
V_C